Building a Sustainable Cybersecurity Culture

Ulil Surtia Zulpratita
Ai Rosita
Sulianta Ferry
Fitrah Rumaisa
Sy.Yuliani
Eka Angga Laksana

DOI: https://doi.org/10.37178/ca-c.23.1.157

***Ulil Surtia Zulpratita**, University of Widyatama, Bandung, Indonesia*
Email: ulil.zulpratita@widyatama.ac.id

***Ai Rosita**, University of Widyatama, Bandung, Indonesia*
Email: ai.rosita@widyatama.ac.id

***Sulianta Ferry**, University of Widyatama, Bandung, Indonesia*
Email: feri.sulianta@widyatama.ac.id

***Fitrah Rumaisa**, University of Widyatama, Bandung, Indonesia*
Email: fitrah.rumaisa@widyatama.ac.id

***Sy.Yuliani**, University of Widyatama, Bandung, Indonesia*
Email: sy.yuliani@widyatama.ac.id

***Eka Angga Laksana**, University of Widyatama, Bandung, Indonesia*
Email: eka.angga@widyatama.ac.id

Abstract

Cyberattacks are currently the quickest developing wrongdoing on a worldwide scale. Monetary losses from cybercrime surpass the total misfortunes brought about from the worldwide trade of every illegal drugs. Henceforth, it shocks no one that people and associations working on the web live in dread of potential hacking situations and data breaches. Beside monetary misfortunes, such types of digital assaults can prompt standing harm also. Human oversight and cyberattacks are inseparably connected. The most fragile link in cybersecurity is the human factor. As cybercriminals keep on embracing new advancements and assault systems, associations should adjust their way to deal with cybersecurity. A strong security culture not just interfaces with the everyday techniques, yet in addition characterizes what security means for the things that association provides to other people. Those contributions might be products, services, or solutions; however, they should have security applied to all parts and pieces. A sustainable security culture is relentless. It is not a once-a-year occasion, it is behavior, which is however embedded in all that we do.

***Keywords:** Cyberattacks, cybersecurity, cybersecurity awareness, security culture, human firewall.*

INTRODUCTION

We live in the data age where cybersecurity stands out enough to be noticed. Not a day passes by without news about network edge breaks, cyber-espionage, ransomware assaults and data leaks. This has prompted partnerships putting huge time and assets into attempting to relieve these dangers. For organizations and consumers, the significant harms of a break can be quite disastrous. These can have broad impacts which those concerned can relate straightforwardly to monetary effect. In any case, does this lessen the significance of actual security frameworks and legitimize not staying up with the most recent accessible advances? Numerous in the actual security business feel that most associations are happy with essential measures. Also, in different cases, an absence of legitimate danger evaluation abilities prompts disappointment in embracing a comprehensive way to deal with security.

Security items and practices ordinarily disregard the most central component of an association: the user. An overview by Willis Tower Watson uncovered that almost 90% of cyberattacks traced back to human error or human behavior [1]. This implies invigorating a network safety culture is similarly just about as significant as online protection insurance. It very well may be hard for Chief Information Security Officers (CISOs) to decide if they have a solid cybersecurity culture. Today, cybersecurity culture is almost difficult to evaluate as there is an absence of devices to quantify and deal with its viability. Without this capacity, CISOs face hardships in working with the important changes expected to work on their association's way of life. The associations who have effectively invigorated an online protection culture have seen an essentially diminished danger of a significant information break. With the new standard of a disseminated labor force bringing an entirely different assault of safety chances focusing on representatives, it's currently more significant than any other time that associations are engaged with an answer that forms and supports a solid cybersecurity culture [2].

To foster a cybersecurity culture, associations should have the option to define security culture, understand how to construct a security cultural model, and managing cultural.

THE IMPORTANCE OF CYBERSECURITY AWARENESS

As our reality turns out to be more associated through headways in innovation, hacking techniques and digital assaults are progressing as well. Business activities depend intensely on innovation, just as client care, bookkeeping, correspondences, and that's just the beginning. To try not to set off any cautions, cybercriminals have gotten savvier at creating tricks and assault vectors to deceive casualties without disturbing business activities. Cybercrime is not disappearing[3].

1. Cybersecurity Threats

A cyberthreat is a malicious and conscious assault by an individual or association to acquire unapproved admittance to one more person's or alternately association's organization to harm, disturb, or take IT resources, PC organizations, licensed innovation, or some other type of touchy information. As indicated by Verizon's 2020 Data Breach Investigations Report (DBIR), 86% of network safety breaks were monetarily roused, and 10% were spurred by espionage.

The most common way of staying aware of new advances, security patterns and danger insight is a challenging effort. It is fundamental to shield data and different resources from cyberthreats, which take many structures. While the sorts of digital dangers keep on developing, there are the absolute generally normal and pervasive cyberthreats that present-day associations need to know. They are as per the following:

a. Malware short for malicious software, is a broad term for viruses, worms, trojans and other dangerous PC programs software engineers use to release annihilation and access sensitive information. Cybercriminals generally use it to isolate data that they can use over losses for financial advantage. That data can go from money related data to clinical benefits records, to individual messages and passwords—the possible results of what sort of information can be compromised have gotten endless.

b. Ransomware is a continually creating kind of malware expected to encode records on a device, conveying any archives and the structures that rely upon them unusable. Threatening performers then solicitation convey as a trade-off for unscrambling. Ransomware performers routinely target and find ways to sell or break exfiltrated data or affirmation information if the result isn't paid. Recently, ransomware scenes have gotten continuously dominating among the Nation's state, local, tribal, and territorial government elements, and basic foundation associations.

c. SQL injection attack - SQL is an abbreviation for Structured Query Language, and a SQL assault is one of the most seasoned cybersecurity breaks. In SQL we make queries. In this manner, in the SQL injection danger, the aggressor sends a noxious inquiry to the gadget (a PC, telephone, and so forth) or a worker. The worker is then compelled to uncover touchy data.

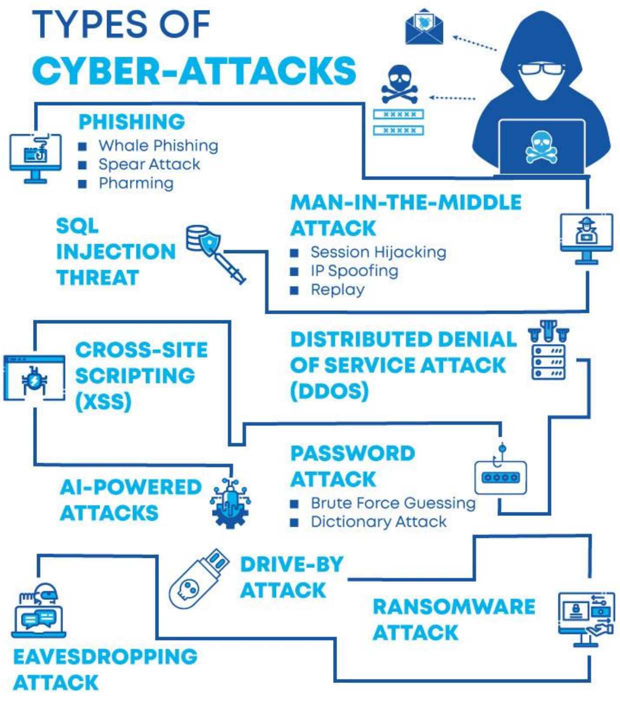

Figure 1. Types of cybersecurity threats

d. Phishing is a cybercrime wherein a goal or targets are reached by email, telephone, or text by someone behaving like a bona fide establishment to bring individuals into giving sensitive data like unmistakable information, banking and charge card nuances, and passwords. The information is then used to get to huge records and can achieve extortion and financial adversity. There are different sorts of phishing we should think about, for instance, email phishing, spear phishing, vishing, whaling, smishing, CEO fraud, pharming, and so forth.

e. Cross-site scripting (XSS) is a digital assault where an assailant sends pernicious code to a trustworthy site. An assault can happen just when a site permits a code to join to its own code. The aggressor packages together two scripts and ship off the person in question. When the content executes, the assailant gets a treat. With this kind of digital assault, programmers can gather delicate information and screen the exercises of the person in question.

f. Distributed Denial of-Service (DDoS) attacks are those where various systems upset the traffic of an assigned structure, similar to a specialist, site or other association resource. The aggressor besieges the framework or worker with high-volume traffic, that its transfer speed and assets can't deal with. Henceforth, they cannot react to asks for. It doesn't normally bring about data fraud or loss of indispensable data. Nonetheless, it will cost truckload of cash to get the worker running once more.

g. Advanced persistent threats (APTs) are drawn out assigned attacks in which an attacker enters an association and stays undetected for huge timespans with the hope to take data.

h. Man-in-the-middle attacks are tuning in attacks that incorporate an assailant impeding and giving off messages between two social events who acknowledge they are talking with each other. Man-in-the-middle is by a wide margin the trickiest assault by hoodlums. Weak WiFi associations and correspondence lines are the least demanding intends to do this security break. The three normal kinds of man-in-the-middle assault are: meeting seizing, IP parodying, and replay.

i. Other cyberthreats are including password attack, eavesdropping attack, AI-powered attack, drive-by attack, and zero-day attack.

Figure 2 shows the distinguish of cyber-attacks sources, to get where is this threat coming from, who has done this and why. A portion of the normal source of cyberthreats include State-sponsored, Terrorists, Industrial spies, Organized crime groups, Hackers, Hacktivists, Malicious insider, Cyber espionage.

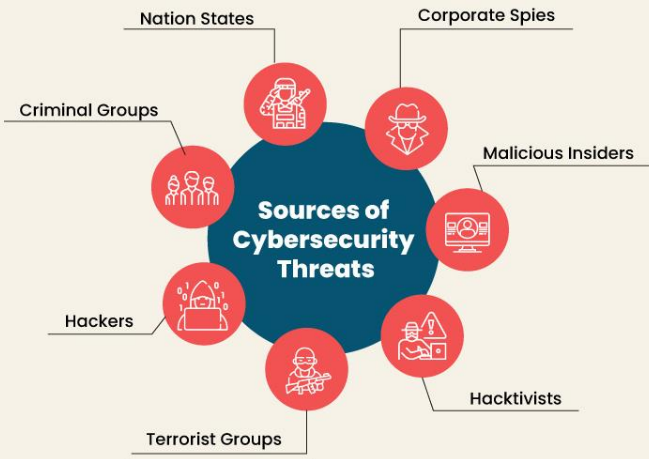

Figure 2. Source of Cyber-attacks

2. Cybersecurity

Cybersecurity is the utilization of advancements, cycles, and controls to ensure frameworks, organizations, projects, gadgets, and information from digital assaults. It plans to lessen the danger of digital assaults and ensure against the unapproved abuse of frameworks, organizations, and advances. It is regularly mistaken for data security. Cybersecurity centers around shielding computer frameworks from unapproved access or being generally harmed or made unavailable. Data security is a more extensive classification that hopes to ensure all data resources, regardless of whether in printed copy or advanced structure.

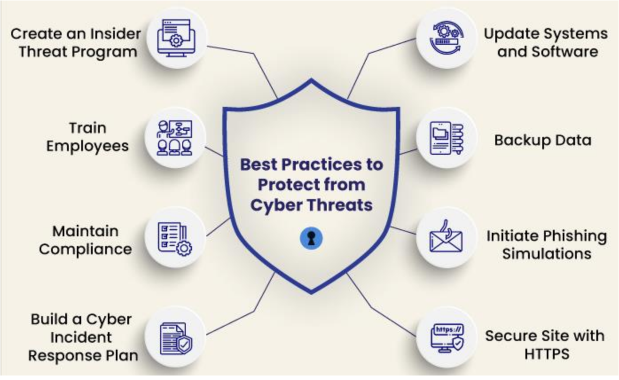
Best Practices to Protect from Cyber Threats
Create an Insider Threat Program
Train Employees
Maintain Compliance
Build a Cyber Incident Response Plan
Update Systems and Software
Backup Data
Initiate Phishing Simulations
Secure Site with HTTPS

Figure 3. Best practices to protect from cyberthreats

As cybercriminals keep on embracing new innovations and assault procedures, associations should adjust their way to deal with online protection. Figure 3 shows some network safety best practices that assist our association with getting ready digital dangers and guarantee business coherence.

As dependence on computerized innovations keeps on expanding, digital assaults have gotten excessively complex. Subsequently, associations that depend on old fashioned online protection methodologies leave themselves helpless against a potential cyberattack. To forestall these dangers, associations should refine their network protection program. A powerful online protection program can assist associations with disturbing assaults as they happen, diminish recuperation time, and contain future dangers.

3. Cybersecurity Awareness

For some foundations, cybersecurity awareness is fundamental to forestall expensive data fraud and organization hacks that can obliterate any organization or person's standing. Aside from executing firewalls and refined IT conventions, organizations currently consider it imperative to increase the capacities of their IT work force by means of courses and such. All things considered, 80% of information breaks can undoubtedly be forestalled by rehearsing digital cleanliness [3].

What drives cybersecurity awareness forward is the developing number of individuals unconscious of most cyberattack strategies. A report by Infosec demonstrates that about 97% individuals on the planet can't recognize a phishing email, while 1 of every 25 individuals snap such messages, along these lines, succumbing to cyberattacks[4] . Beside this, cybercriminals now resort to further developed and innovative types of phishing and malware contaminations.

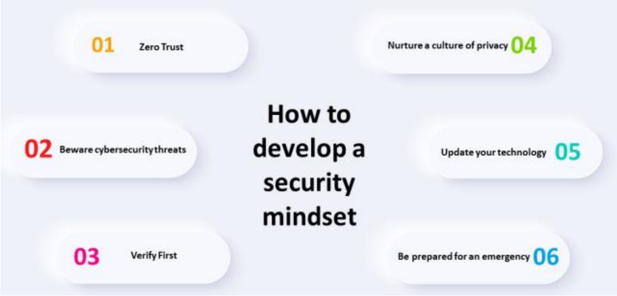
01 Zero Trust
02 Beware cybersecurity threats
03 Verify First
How to develop a security mindset
Nurture a culture of privacy 04
Update your technology 05
Be prepared for an emergency 06

Figure 4. Six ways to develop an individual security mindset

Figure 4 shows how to develop a security mindset. Because cybersecurity is not only about tools and techniques, but also about a mindset. Tools, procedures, and techniques to send those security controls proliferate in any case cybersecurity experts need to take on a particular mindset to ensure their association information and foundation best. The requirement for staff to adjust their reasoning and embrace a considerably more careful way to deal with cybersecurity is a higher priority than at any other time as numerous associations have detailed an expansion in digital assaults during the Covid-19 pandemic.

Thus, cybersecurity awareness could assist with forestalling the invasion of dangers and assaults. A few associations have begun to carry out the consolidated utilization of web-and homeroom-based techniques and visual guides for online protection mindfulness preparing and advancements. On top of this, organizations currently decide zeroing in on how representatives handle and offer classified corporate information.

DEVELOPING A CYBERSECURITY CULTURE

Cybersecurity culture is that slurry of variables that set somebody in a place to do (or more regularly, not do) that network safety conduct. For what reason does an association require a security culture? The essential answer is something that where it counts, we know. In any framework, people are consistently the most vulnerable hole. Security culture is principally for the people, not for the PCs. The PCs do precisely what we advise them to do. The test is with the people, who click on things they get in email and accept what anybody advises them. The people need a system to get what the proper thing is intended for security. As a rule, people inside your association need to make the best decision—they simply should be educated[5].

Making a culture around cybersecurity awareness in the working environment doesn't imply that we will be totally killing the danger of information burglary or digital crime to our business. Malware has prospered, turning out to be increasingly more modern as each new strand is created, and we hope to see the development and development of digital dangers and malware to multiply. Panda security recognized more than 225,000 new malware strains each day in the main quarter of the year 2015, with tops coming to 500,000. This record-breaking figure addresses a 40 percent increment over Q1 2014 and is well over the normal for the whole year, which remained at around 205,000 new malware tests each day. It is essential to feature that these were the strains that cybersecurity companies had found and recognized. As new strains of malware develop, ventures need to guarantee that they're executing the fitting safety efforts, teaching their representatives, and taking out any shortcomings that make them defenseless against an assault. Human blunder is a terrible adventure that can prompt fines and serious business harm[6].

Cybersecurity culture inside an association is the aggregate online protection conduct, all things considered. To foster a powerful gathering or cultural cybersecurity model, associations should use a singular cybersecurity conduct model. In view of Fogg's exploration, the essential parts of a singular conduct model can be partitioned into three head classifications: Motivational, Ability, and Nudge.

An association can handle these factors - Motivation, Ability, and Nudge - to work with individual changes in representatives' conduct. The graphs displayed in Figure 5 helps to clarify the different elements that impact the online protection conduct of a singular representative.

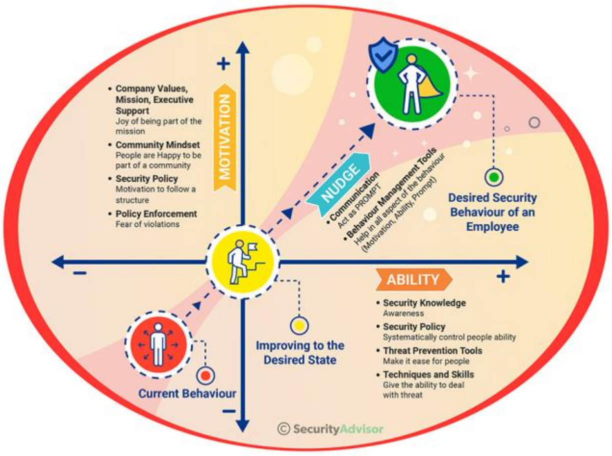
• Company Values, Mission, Executive Support
Joy of being part of the mission
• Community Mindset
People are Happy to be part of a community
• Security Policy
Motivation to follow a structure
• Policy Enforcement
Fear of violations
+
MOTIVATION
−
NUDGE
• Communication
Act as PROMPT
• Behaviour Management Tools
Help in all aspect of the behaviour (Motivation, Ability, Prompt)
Desired Security Behaviour of an Employee
−
ABILITY
+
• Security Knowledge
Awareness
• Security Policy
Systematically control people ability
• Threat Prevention Tools
Make it ease for people
• Techniques and Skills
Give the ability to deal with threat
Improving to the Desired State
Current Behaviour
−
© SecurityAdvisor

Figure 5. Employee cybersecurity behavior model [7]

An association's security culture requires care and taking care of. It isn't something that fills in a positive manner naturally. We should put resources into a security culture. A reasonable security culture is greater than simply a solitary occasion. At the point when a security culture is feasible, it changes security from a one-time occasion into a lifecycle that creates security returns for eternity.

CONCLUSION

Numerous associations have the opinion that the security office is liable for security. Sustainable security culture necessitates that everybody in the association is holding nothing back. Everybody should feel like a security individual. This is security culture for everybody. Security has a place with everybody, from the leader staff to the hall ministers. Everybody possesses a piece of the organization's security arrangement and security culture.

Cybersecurity is an intrinsic risk management that should be incorporated into the center of each employee, product, and service. The times of depending entirely on border security are disappearing. Organizations need to embed security by plan and default into their endeavor DNA. This implies revamping the way of life and standards of conduct of representatives to set up security as a guiding principle, which has turned into an obligation basically as significant as taking a gander at the latest patterns in protection advancements and the following must-have on the CISO's plan. Many organizations have as of now embraced awareness campaign and may have set up strategies and systems to turn out to be more protective. Today, setting up a cybersecurity mindset that assists employee with intuition like an assailant has gotten essential.

ACKNOWLEDGMENT

This work is supported by Widyatama University.

REFERENCES

1. Hargreaves, T., *Practice-ing behaviour change: Applying social practice theory to pro-environmental behaviour change.* Journal of consumer culture, 2011. **11**(1): p. 79-99.DOI: https://doi.org/10.1177/1469540510390500.
2. Reegård, K., C. Blackett, and V. Katta. *The concept of cybersecurity culture*.

3. de Bruijn, H. and M. Janssen, *Building cybersecurity awareness: The need for evidence-based framing strategies.* Government Information Quarterly, 2017. **34**(1): p. 1-7.DOI: https://doi.org/10.1016/j.giq.2017.02.007.
4. Kim, L., *Cybersecurity awareness: Protecting data and patients.* Nursing management, 2017. **48**(4): p. 16-19.DOI: https://doi.org/10.1097/01.NUMA.0000514066.30572.f3.
5. Gcaza, N. and R. Von Solms, *A strategy for a cybersecurity culture: A South African perspective.* The Electronic Journal of Information Systems in Developing Countries, 2017. **80**(1): p. 1-17.DOI: https://doi.org/10.1002/j.1681-4835.2017.tb00590.x.
6. Alshaikh, M., *Developing cybersecurity culture to influence employee behavior: A practice perspective.* Computers & Security, 2020. **98**: p. 102003.DOI: https://doi.org/10.1016/j.cose.2020.102003.
7. Anwar, M., et al., *Gender difference and employees' cybersecurity behaviors.* Computers in Human Behavior, 2017. **69**: p. 437-443.DOI: https://doi.org/10.1016/j.chb.2016.12.040.